

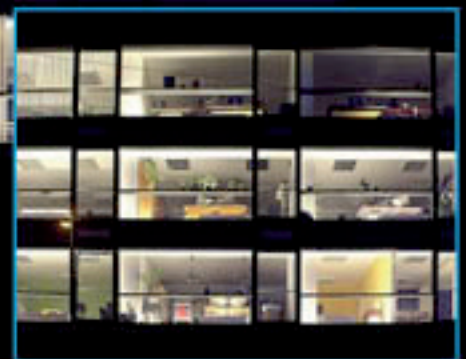
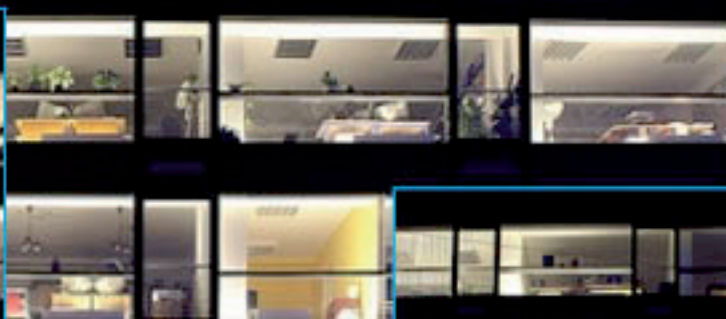
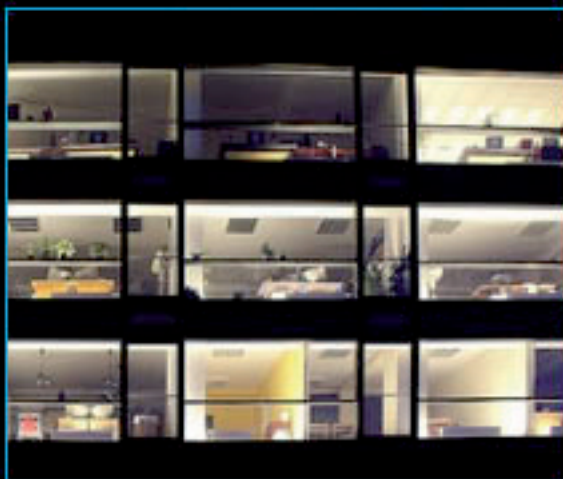
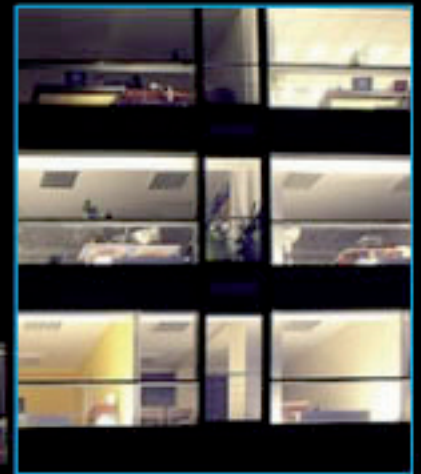
VIGIE

N 32 Février 2010

Spécial



RENAULT



ICOMTEC.VIGIE@GMAIL.COM
HTTP://VIGIE.ICOMTEC-PRO.FR



IE
Poitiers

Les leçons à tirer de l'affaire Renault

L'affaire Renault fait la Une des médias depuis quelques semaines maintenant. Cette affaire d'espionnage industriel a au moins eu le mérite que l'on entende parler d'intelligence économique dans les journaux. Cet événement qui a touché l'industrie automobile a permis de montrer le retard conséquent que la majorité des entreprises françaises ont pris par rapport à leurs homologues, notamment les Etats-Unis. Cela a également mis en avant le cruel manque de moyens que possède la justice pour juger ces délits d'espionnage industriel. Tout en revenant sur l'affaire qui touche la marque au losange, il est intéressant de voir que des précédents ont récemment, sans pour autant que des décisions fortes venant de l'Etat n'aient été prises pour changer la donne.

Outre son illégalité, le vol d'informations pour les concurrents est un précieux gain de temps et d'argent. Dans des secteurs hautement compétitifs comme l'aéronautique, l'automobile, l'énergie et l'industrie pharmaceutique, des acteurs malveillants ont recours à de telles pratiques car la bonne information dans une course à l'innovation permet d'accélérer les projets en cours. Ainsi, il vaudrait presque mieux faire chanter un ingénieur d'un concurrent et le payer des sommes considérables plutôt que d'investir 10 milliards en R&D. En effet, les fonds versés dans la recherche et développement sont impressionnants, et ce chiffre en milliards d'euros. Renault qui ambitionne d'être le premier constructeur à proposer des véhicules zéro émission, a investi plus de 4 milliards d'euros dans le projet électrique, rien que pour la production de la Leaf (la voiture électrique stratégique de Renault-Nissan). Carlos Ghosn, PDG de Renault, affirmait d'ailleurs lors de son interview aux journées de conférences "Le Web'10", que l'industrie automobile avait toujours souhaité l'apparition de la

voiture électrique. Seulement, la technologie de la batterie ne le permettait pas. Aujourd'hui, oui. A l'approche de la pénurie de ressources pétrolières, les derniers enjeux concurrentiels du secteur de l'automobile se jouent donc sur l'innovation électrique et la puissance des batteries. Autant dire, que si un concurrent parvient à obtenir les informations sur cette technologie, toute la longueur d'avance qu'aurait pris le groupe serait réduit à rien et le concurrent en question aura réaliser plusieurs milliards d'euros d'économie.

Les conséquences de l'espionnage industriel sont alors bien malheureuses pour celui qui les subit. Comme l'explique Bernard Lage dans le Figaro, *« une fuite d'informations relatives à la stratégie, la politique commerciale, le lancement de nouveaux produits ou encore l'innovation peuvent occasionner à l'entreprise des pertes de marchés, une décroissance des ventes, un retard important par rapport à des concurrents et autres avaries préjudiciables. »*

On retrouve plusieurs termes associés à tort ou à juste titre avec l'espionnage industriel, tels qu'espionnage économique, risques d'affaire, secret d'entreprise, contre espionnage, fuite d'information.



http://www.dailymotion.com/video/xg1rgk_interview-l-innovation-vue-par-carlos-ghosn-renault_news

<http://blog.lefigaro.fr/crequy/2011/01/la-revelation-de-pratiques-despionnage.html>



1. L'affaire Renault

Des informations hors-cadre

Cinq mois d'enquête interne. Depuis la fin août dernier, une « alerte éthique » a été lancée et portée à la connaissance du comité de déontologie du groupe (ce département peut recevoir des plaintes sans en informer aucun autre service et peut donc décider de diligenter une enquête). Dès lors, une enquête a été menée en interne. Cette investigation a donc révélé que des informations stratégiques pour l'entreprise auraient été transmises hors des murs de la firme. Selon « Le Parisien », la principale fuite porterait sur les méthodes de fabrication des batteries et des moteurs des prochaines voitures du constructeur. Cela dit, ce dernier est pour le moins évasif quand il s'agit d'évoquer lesdites informations. Patrick Pélata, le numéro deux du groupe, oscille le chaud et le froid. Selon lui, la société est « victime d'une filière organisée internationale », et interrogé par Le Monde, ajoute qu'elle est « face à un système organisé de collecte d'informations économiques, technologiques et stratégiques pour servir des intérêts situés à l'étranger ». Cependant, M. Pélata tient à rassurer en expliquant qu'« aucune pépite technologique, stratégique [...] n'a pu filtrer en dehors de l'entreprise ». Toutes les recherches réalisées par le groupe et les différents brevets sont donc conservés en lieu sûr. Mais quelles sont alors les informations ayant pris la porte ? Toujours selon le numéro deux de la société, il s'agirait d'informations sur l'architecture des véhicules, ainsi que sur les coûts et le modèle économique de la construction des futures voitures électriques de la marque.

Cette enquête a donc révélé quelles sont les informations qui avaient pris la tangente, mais aussi qui serait à l'origine de ces fuites. Trois cadres du technocentre de Guyancourt, sont suspectés d'avoir outrepassés le simple cadre de leur travail. Un des membres du comité de direction, la personne en charge des avant-projets et le directeur de programme adjoint du véhicule électrique. Tous nient en bloc les accusations. Deux d'entre eux ont d'ailleurs porté plainte pour dénonciation calomnieuse, mais cela n'y a rien fait, ils n'ont aujourd'hui plus accès à leurs ordinateurs de travail, leurs salaires ont été suspendus et ils sont priés de ne plus remettre les pieds dans leurs bureaux.



Des informations en partance... mais pour quelle destination ?

Apparemment, Renault a l'air convaincu de la culpabilité de ses trois cadres, mais le fait est, que le flou règne autour de la destination qu'ont prise les informations. Dès que Patrick Pélata, a parlé de filière internationale organisée, les yeux se sont tout de suite tournés vers le géant chinois. Selon le Figaro, d'importantes sommes d'argent auraient été déposées sur les comptes de deux des cadres impliqués dans l'affaire. Ces sommes proviendraient d'une société chinoise de distribution d'électricité. Cela dit, les montants donnés par le quotidien semblent peu probable, puisque l'on parle de 130 000 € et de 500 000 €. Des valeurs plutôt faibles, au vue des salaires touchés par les salariés arrivés à un tel niveau de responsabilités. Difficile donc de croire à cette version des faits, eu égard aux risques encourus par ces personnes. Comme l'explique différents experts de l'espionnage industriel, il y a d'autres possibilités de payer le vol d'informations au sein d'une entreprise aussi importante que peut l'être Renault. L'organisme commanditaire peut décider d'exfiltrer le « traître » pour lui offrir une deuxième carrière, tout en lui offrant des biens matériels pour qu'il s'installe confortablement dans le pays.





Cette piste chinoise, vraie ou fausse, ne fait en tout cas pas plaisir à la puissance communiste. Pékin a jugé ces accusations comme « totalement sans fondements, irresponsables et inacceptables ». Afin d'éviter une montée en puissance et un refroidissement des liens Sino-français, François Baroin a expliqué qu'« il n'y avait pas d'accusation officielle de la France et du gouvernement français à l'égard d'aucun pays aujourd'hui ».

On peut également envisager un autre scénario, un peu moins hollywoodien celui-ci : la piste interne. Cette histoire qui a pris des allures d'affaire d'Etat, pourrait tout simplement être la résultante de troubles entre différents salariés du groupe. Histoires de vengeance, d'égo ou de jalousie, qui amènent à ce genre d'actions, dans le but de ternir l'image de certains acteurs au sein de la technopole.

Tapage médiatique et image de marque

Renault subit de plein fouet les commentaires à tout va de la presse. Dans les prochains jours, la grande difficulté de Renault sera de détacher son nom de cette affaire. La volonté initiale de l'entreprise était d'ailleurs de ne pas l'ébruiter car les tapages médiatiques de cet ordre altèrent la réputation des marques. Un cas d'espionnage industriel est bien souvent tu pour ne pas inquiéter fournisseurs et clients. Insuffisamment prudent, un client pourrait songer ainsi à la gestion de ses données au sein de l'entreprise (Qu'en est-il de mes données dans cette affaire ? Des informations ont-elles été communiquées à mon sujet ?). En interne, un vent de pessimisme ou d'inquiétude souffle sur la tête des salariés (Qu'en sera-t-il de mon emploi ?). De même que de futurs partenaires potentiels se montreraient soudainement dubitatifs, « *pouvant estimer que les conséquences de ces fuites pourront impacter leur propre activité. Le risque d'image pour l'entreprise est un facteur à ne surtout pas négliger* » (Bernard Lage) .

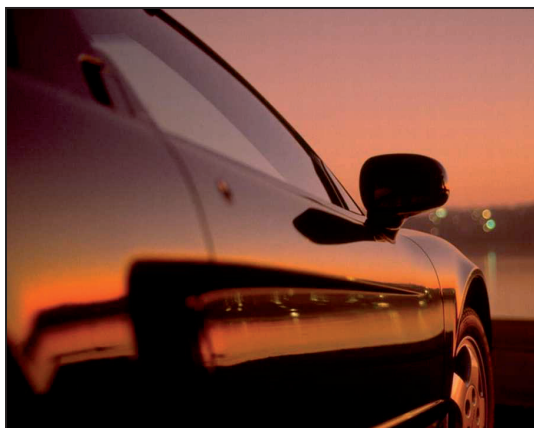
Christophe Casalegno (Intelink.info, Digital-Network) estimait que « par pudeur, personne n'ose avouer qu'il a subi un dommage à ce propos, d'autres mettent dix ans pour s'en apercevoir ! Par conséquent, aucune statistique n'est publiée faute d'obtenir des données » . Nous reviendrons cependant sur les quelques chiffres communiqués.

2. Quelques cas historiques d'espionnage industriel

Renault n'est pas le premier à connaître une affaire d'espionnage industriel. On peut citer l'un des cas les plus célèbres en matière d'espionnage industriel, l'affaire Tupolev / Concorde. Quand il fut arrêté, Sergei Pavlov, alors directeur d'Aeroflot, (compagnie aérienne nationale russe), seule compagnie à avoir exploité le fameux Tupolev, aurait été en possession de plans des freins, du train d'atterrissage de l'appareil français. Et les similitudes entre les deux appareils étaient tellement importantes que l'on surnomma le Tupolev, le « ConCORDski ».

Mais, plus récemment, deux autres grands noms du secteur de l'automobile ont eux aussi été touchés par des vols d'informations : Valeo et Michelin. En 2005, Valeo, concepteur, fabricant et vendeur de composants pour l'automobile, a poursuivi en justice une jeune stagiaire chinoise. Cette dernière s'était emparée entre février et avril 2005 de fichiers informatiques confidentiels lors d'un stage qu'elle avait réalisé chez l'équipementier. La stagiaire aurait sorti des données de l'entreprise pour les emmener chez elle. Elle explique, qu'elle ne savait pas que toutes ces informations étaient confidentielles, puisqu'elle y avait accès librement via l'intranet de la société.





Le fabricant de pneus Michelin, a poursuivi un de ses anciens cadres, qui avait tenté de vendre des données confidentielles à Bridgestone, son concurrent principal. Heureusement pour Michelin, le Japonais a joué franc-jeu en alertant le Français des offres de ventes d'informations provenant du salarié, empêchant ainsi toute transaction. L'auteur des faits, un ancien ingénieur a expliqué, que tout cela n'était qu'un jeu pour lui. Un jeu qui aurait tout de même pu lui rapporter 115 000 €, son prix de vente pour les informations.

Devant les montants et les enjeux de ces vols d'informations, on aurait pu s'attendre à ce que la justice, rende un jugement sévère. Pourtant, dans les deux cas, les personnes incriminées ne sont pas restées bien longtemps derrière les barreaux. Dans l'affaire Valeo, le tribunal de Versailles balaye l'espionnage industriel et requalifie le jugement en « abus de confiance ». Li Li, la jeune chinoise a été condamnée à un an de prison, dont deux mois ferme. L'ancien cadre de Michelin n'est quant à lui même pas passé par la case prison, en étant condamné à deux ans de prison avec sursis. ‘

3. IE / espionnage, amalgame ?

Nous avons tous, étudiants en IE ou professionnels confirmés, été confrontés aux raccourcis mentaux et à l'association triviale de nos pairs réduisant simplement l'intelligence économique à de l'espionnage industriel. L'association des deux domaines semble plus évidente dans l'esprit du grand public, l'espionnage industriel n'étant pas né d'aujourd'hui, contrairement à l'intelligence

Source : B. Martinet, Y-M. Marti. *L'intelligence économique*.
Paris : les Editions d'Organisation, 1995. p137

LA FIN (INFORMATION RECHERCHEE)	information noire (fermée, secrète)	interdit	interdit	espionnage (au sens strict)
	information grise (semi-ouverte)	intelligence économique	intelligence économique	bêtise dangereuse
	information blanche (ouverte)	intelligence économique	bêtise dangereuse	bêtise dangereuse
		ouverts	organisés et déontologiques	illégaux
LES MOYENS UTILISES				

<http://blog.lefigaro.fr/crequy/2011/01/la-revelation-de-pratiques-despionnage.html>

<http://www.spyworld-actu.com/spip.php?article1474>



économique formalisée il n'y a qu'une quinzaine d'années.

Les différences entre espionnage industriel et IE

Informations blanches, grises et noires... Dans le travail d'un expert, entre 5 et 10% des informations sont noires. Plus l'expert avancera dans ses recherches sur la concurrence, plus les informations

seront sensibles, et se concentreront dans ces 5-10%. « *Ce sont souvent les 10% restants qui seraient vitaux pour aboutir à une bonne compréhension de la stratégie du concurrent. Or, ceux-ci ne peuvent provenir que de sources « grises », comme l'espionnage industriel* » (Joëlle Noailly). Les 5 à 10% d'informations inaccessibles renferment bien entendu ce qui intéresse le plus les espions économiques : la fourchette de prix dans laquelle se trouve un concurrent lors d'un appel d'offres international, le volume d'avions possiblement vendus, etc .



IE Love PME reprenait une série de différences intéressantes :

Etant donné la quantité d'informations blanches disponibles, le champ d'analyse du chargé d'IE et le travail de traitement des données sont donc beaucoup plus larges que celui de l'espion qui se focalise sur les 10% interdits. L'environnement informationnel global de l'IE est beaucoup plus global (acteurs, marchés, technologies, brevets, salons, médias généralistes et la presse spécialisée) tandis que l'espionnage industriel s'informe sur un élément précis.

D'autre part, les coûts engendrés ne sont pas de même taille. L'espionnage industriel investit des sommes faramineuses pour acquérir l'information noire, sommes justifiées par le caractère illégal et risqué des actions. L'IE est en revanche un investissement plus étalé dans le temps.

D'autre part, la société espionne aurait bien des difficultés à justifier ses actes si le scandale venait à être révélé et serait discréditée par l'opinion publique. Alors qu'une société utilisant des moyens légaux, des moyens venant de l'IE, n'aurait rien à se reprocher puisqu'elle aura(it) travaillé sur de l'information blanche.

Enfin, une des dernières différences réside dans la diffusion des informations faite en interne. Une information d'IE sera plus aisément diffusée aux différents employés, contrairement à une information issue de l'espionnage, dédiée à un nombre très restreint de responsables.

NOAILLY, Joëlle. « L'Espionnage Industriel Au Cœur De La Guerre Mondiale Du Renseignement Economique », 1996 – 1997. <http://strategie.free.fr/analyses/meminfow.pdf>

http://www.dailymotion.com/video/xbt3qn_espionnage-industriel-communication_school

<http://www.ielovepme.com/strategie/56-une-confusion-l-electrique-r-entre-intelligence-economique-et-espionnage-economique.html>

<http://www.portail-ie.fr/dernieres-actualites/dernieres-actualites/laffaire-renault-entre-amalgames-et-emballement-mediatique.html>



Enfin assez peu d'amalgames dans la presse sur l'affaire Renault

Contrairement aux propos avancés dans l'article "L'affaire Renault : entre amalgames et emballement médiatique" du Portail de l'IE, il semblerait que l'amalgame IE/espionnage s'estompe cependant. Bien entendu, certains d'entre eux ont fait quelques bourdes, mais assez peu, comparée à la masse d'informations sorties sur l'affaire Renault. En terme de proportions, les journalistes auraient cette fois-ci dissocié plus habilement les deux concepts. Cette plus nette dichotomie est très certainement dû au fait de la réactivité des grands noms de l'IE, qui se sont immédiatement mis sur le devant de la scène au moment où le scandale éclatait. Pendant que Christian Harbulot alignait les interviews (AFP, C dans l'air, l'Expansion, France Info,...), on retrouvait Alain Juillet, Bernard Carayon, Ali Laïdi, Peer de Jong,... occupés de leur côté avec d'autres journalistes. Tous étaient au rendez-vous pour rappeler le contexte de guerre économique, et que la culture française est une des seules cultures à dévaluer les risques et à sous-estimer les tensions de la concurrence.

Était-ce l'occasion de mettre en avant les cabinets d'IE et les audits privés ? Peut-être aussi. En plus de devoir défendre le bataillon de la profession, l'occasion de promouvoir l'expertise des confrères dans ce genre de situations semblait se présenter.

Qu'aura retenu le grand public ? Le manque de sûreté en contexte économique, certes. Mais aura-t-il saisi les nuances entre contre espionnage, sûreté et sécurité ? Un point sur lequel le corps de métier n'aura pas assez insisté est bien que le rôle de l'intelligence économique, en plus de se déployer dans un cadre légal correct contrairement à son "ennemi" l'espionnage industriel, est de mettre en place les mesures de défense et de contre offensive pour sauver l'intégrité de l'entreprise !

4. L'ampleur du phénomène

Un nombre de cas alarmants ?

Plusieurs professionnels s'accordent pour dire que l'espionnage économique ne cesse de s'accroître, et ce, au détriment des entreprises françaises.

Interrogé par le Journal du Dimanche, Olivier Buquen affirmait que "le nombre des incidents survenus sur le territoire français, que nous recensons depuis cinq ans, est alarmant. Il s'élève à plusieurs milliers. Il révèle aussi que tous les secteurs, toutes les régions, et des entreprises de toutes tailles, sont touchés. Le nombre de pays dont les ressortissants se livrent à de l'espionnage industriel est aussi en progression. Le cas Renault illustre donc la nécessité croissante pour toute entreprise de se protéger."

D'un côté, nous trouvons une prétendue masse salariale peu soucieuse de ces risques et d'un autre, une profession qui prétend que le mal est plus répandu que nous ne le pensons, mais incapable de fournir à la presse de véritables preuves. Combien d'attaques subissent les entreprises françaises ? De quel ordre sont-elles ?

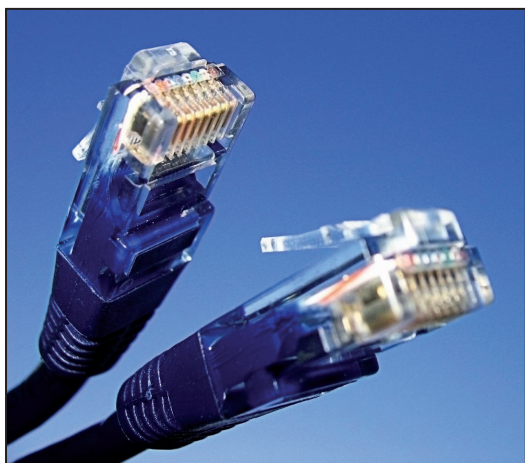


Certains chiffres circulent sur la toile, que VigIE évoque ici à titre indicatif (bien qu'ils soient basés sur des variables incertaines) :

- En 2005, les renseignements généraux français annonçaient qu' "**1 société sur 4 est ou a été touchée par l'espionnage industriel**" .
- En 2006, les renseignements généraux, toujours, recensaient **1 578** vulnérabilités et agressions économiques hostiles à destination d'une neuf centaine d'entreprises.
- **75 %** des entreprises françaises visées par une attaque extérieure sont des PME de moins de 500 salariés
- En 2009, les entreprises allemandes auraient perdu 50 milliards d'euros à cause de l'espionnage industriel chinois, selon Walter Opfermann, spécialiste allemand du contre espionnage.
- Selon un enquête américaines, **48%** des fuites ont été provoquées par un salarié (**+26%** sur un an). Dans **70%** des cas, une personne extérieur est en cause (**-9%** sur un an)
un partenaire commercial est impliqué dans **11%** des cas (**-23%** sur un an)
- Quant aux moyens de diffusion de l'information compromise, il s'agit le plus souvent de **salariés qui ont outrepassé leurs droits** (dans **48%** des cas, **+26%** sur un an).
- Le **piratage** informatique est la cause de **4 fuites sur 10** (en baisse de **24%** sur un an) .

Les français, de grands naïfs ?

Comme vu précédemment, des cas d'espionnage industriel sont révélés d'années en années. Les comportements des entreprises ont-ils changés suite à ces scandales ? Qu'avons-nous retenus des cas d'école ?



Selon Eric Dénécé interrogé par RFI, la philosophie française – probablement issue des Lumières - ne reconnaît pas les logiques d'affrontement. Dans l'esprit des anglo-saxons, « *L'économie, c'est la guerre et tous les coups sont permis* ». Techniques de destabilisation, d'espionnage, d'approche issues du monde du renseignement, fausse tentative de recrutement d'une entreprise adverse, pièges lancés à un cadre supérieur,... Non, les français sont moins enclin à pratiquer les méthodes d'espionnage industriel, ce qui impose d'être beaucoup plus prudent. Une prudence qui s'apprend au cours de stages de sensibilisation et de formation des salariés aux pratiques de la concurrence .

<http://www.lejdd.fr/Economie/Industrie/Actualite/Olivier-Buquen-delegue-interministeriel-a-l-Intelligence-economique-revient-sur-l-affaire-Renault-252627/>

<http://www.spyworld-actu.com/spip.php?article2848>

<http://www.netpme.fr/propriete-intellectuelle/1214-intelligence-economique-comment-protoger-information-strategique.html>



VIGIE@POITIERS-IE.NET
HTTP://VIGIE.COMTEC-PRO.FR



Nicolas Moinet parlait d'ailleurs de "carence culturelle" dans son article des Echos, appelant ainsi à la nécessité de faire témoigner les autres chefs d'entreprise et de sensibiliser à la sécurité économique. Il ajoute que *"la protection des informations ne peut se développer dans les entreprises que dans le cadre plus large d'une politique d'intelligence économique qui implique l'ensemble des salariés à tous les échelons et favorise un management de l'information transversal qui décroïssonne les services. Car la sécurité est une histoire de posture avant d'être une question de procédures."*

Alain Juillet déclarait de son côté (C dans l'air, Les Echos) que nous devons cesser d'être naïfs. *« Dans cette lutte pour la compétitivité et la survie économique, il n'y a pas d'amis ; il n'y a que des ennemis car chacun voit midi à sa porte ».*

Méthodes d'espionnage : tout est possible

Identifier la cible

La technique élaborée est d'abord l'identification de la cible et l'appréhension de son environnement : son profil, ses réseaux, les raisons de ses déplacements. L'espion cherche également à comprendre les réseaux internes d'une entreprise : il s'agit alors de comprendre les relations d'affinités entre les employés. Eric Delbecque, interrogé par le Nouvel Observateur, explique qu'en cas de rachat, l'espion veut savoir quelles seraient les motivations de chacun et qui pourrait trahir.

Egalement, on cherche les mécontents, ceux qui seraient susceptibles de partir... de manière à leur proposer un poste intéressant pour une seconde carrière (piste évoquée pour l'affaire Renault). Cette identification se fait d'ailleurs en amont, grâce à tout ce que ces mécontents peuvent communiquer, sur les réseaux sociaux notamment. Le mécontentement peut se traduire par un manque de reconnaissance au sein de l'entreprise, de rancœur ou de déception... et peut pousser ces employés à vendre l'information au concurrent.

Faire chanter

Vous n'êtes pas très bon en chant ? Ce n'est pas grave, on cherche simplement les paroles. Vous n'êtes pas extraordinaire ? On vous affirmera que si.

Flatter l'égo de l'autre est probablement ce qui fonctionne le mieux. D'autre part, dans tout ce que vous direz, y compris des banalités, tout ne sera pas forcément exploitable. Mais c'est la reconstitution d'un puzzle d'informations éparses qui permettra d'atteindre la vérité recherchée.

Exemples :

☐ Faux recrutement : un employeur prétend vouloir vous recruter, les questions deviennent de plus en plus précises au cours de l'entretien,... Mais vous n'êtes finalement pas recruté, faute de ne

<http://blog.lefigaro.fr/crequy/2011/01/la-revelation-de-pratiques-despionnage.html>

<http://www.rfi.fr/economie/20110106-espionnage-industriel-mode-emploi>

MOINET, Nicolas. « Seuls les paranoïaques survivent ». Les Echos, 8 janvier 2011

<http://blogs.lesechos.fr/intelligence-economique/nouvel-article-a4731.html>

TATU, Natacha. « Contre espionnage : mode d'emploi ». Nouvel Observateur, 22 – 26 janvier 2011.





pas avoir le profil suffisamment adéquate.

- ☐ Des conversations a priori anodines dans le train
- ☐ Une (trop) charmante stagiaire qui vous pose des questions personnelles
- ☐ Des questionnaires / sondages / enquêtes bidons par téléphone

(Très) bien payer

Toute information a un coût, le silence de la source aussi. C'est donc la source qui fixe son prix. Il ne reste plus qu'à savoir lequel.

On expliquerait la trahison des cadres de Renault par les sommes qu'ils auraient reçues via des comptes à l'étranger. Comme écrit plus haut, les sommes annoncées semblaient insuffisantes par rapport à l'importance des informations stratégiques qui auraient pu être livrées. Mais il se

pourrait que ces sommes soient finalement proportionnelles au faible degré de confidentialité des informations que les cadres auraient fournies.

D'autres méthodes sont utilisées à l'insu de la cible :

- ☐ Fouilles des chambres d'hôtel en votre absence
- ☐ Une clé USB qui traîne, dont on veut vérifier le contenu : or, la clé USB a été placée à un endroit stratégique et contient des mouchards
- ☐ tamponnage, accident provoqué
- ☐ vol d'ordinateur / téléphone au moment où vous tournez le dos.

5. Alors, que faire ?

Objectif légal : protéger le secret industriel

Renault se veut très discret sur cette affaire et ne s'exprime pas sur les pistes envisagées et communiquées par les médias. Le groupe a tout de même porté plainte contre X le 14 janvier, sans doute en raison du tapage médiatique. Mais le droit français étant tellement flou et non adapté à des affaires d'espionnage industriel (il n'y a qu'à voir les faibles sentences prononcées dans les précédentes affaires), l'objet sur lequel porte la plainte est large. Notez plutôt, Renault porte plainte pour : espionnage industriel, corruption, abus de confiance, vol et recel commis en bande organisée (à noter que les noms des trois salariés ne sont pas mentionnés dans la plainte).

Aucun texte de loi n'est réellement efficace pour la protection juridique de l'information. Pour mieux comprendre, à l'heure actuelle, en France, le vol de bien immatériel et donc d'informations, n'est pas punissable par la loi. D'autre part, la justice ne parle d'espionnage que s' « il porte atteinte aux intérêts fondamentaux de la nation ».



Pour changer la donne, Bernard Carayon, député UMP du Tarn a déposé, le 12 janvier dernier une proposition de loi sur le secret des affaires. Le projet de loi rappelle que « la législation actuelle ne permet pas de protéger en amont l'ensemble des secrets d'affaires ». L'idée forte de ce projet est d'établir « une protection juridique efficace et globale de l'ensemble des informations et des connaissances de l'entreprise ». Le texte est directement inspiré du Cohen Act américain, qui instaure outre-Atlantique des peines bien plus sévères que ce que l'on peut connaître dans l'Hexagone. Le projet instaure le vol d'informations dans la loi française. L'article 2 explique que tous les dirigeants ou les salariés qui révèlent ou tentent de révéler une information à caractère économique pourront être poursuivis. Il n'y a plus qu'à espérer que ce projet soit inscrit à l'agenda parlementaire et ensuite voté. Il se pourrait que l'affaire Renault accélère quelque peu le débat.



En interne : prévenir pour guérir

La sécurité relève de la culture d'entreprise. Toute entreprise a un dispositif de sécurité, des règles et des procédures à respecter. Les deux seuls manquements résident dans le peu d'exigence et de motivations des personnels pour respecter ces règles. En effet, leur respect ne va pas de soi et les règles sont parfois détournées pour gagner du temps ou faciliter le quotidien.

Mesures à prendre par l'entreprise

1. Définir sa stratégie de prévention : selon Spyworld, il faut formaliser cette stratégie de prévention par une charte, en contrôler l'application, l'adapter aux événements, valider sa pertinence régulièrement, installer les systèmes adéquats, pratiquer des contrôles techniques réguliers, et ne surtout pas attendre quand le scandale éclate.

2. Rédiger des clauses de confidentialité et des contrats de travail pertinents : les contrats de travail doivent être bien conçus en terme de propriété intellectuelle et de secret. L'exemple anglo-saxon montre d'ailleurs que les secrets de l'employé appartiennent à l'entreprise et que toute information transmise illégalement est sanctionnée d'un licenciement direct sans indemnités.

Quant aux clauses, elles doivent également être signées avec les partenaires, les fournisseurs et les clients.

3. Définir une procédure déontologique : utilisée chez Renault notamment, elle a permis à un de ses salariés de dénoncer un manquement à l'éthique et d'identifier les fuites.





4. Maîtriser la communication d'entreprise : inutile de trop détailler les bilans annuels, les méthodes élaborées dans un appel d'offre, l'état d'avancement d'un projet, y compris dans le journal interne, ou de trop en dire à un journaliste (exemple d'un article sur Renault, annonçant "Les nouveaux prototypes de Renault" rédigé à la suite d'une conversation avec un employé trop bavard).

5. Veiller à sa réputation post-scandale : nous l'avons vu précédemment, un scandale d'espionnage altère l'image d'une entreprise. Il faut donc surveiller ce qu'il sera dit offline et online.

6. Entretenir des rapports avec les services de renseignements : la DCRI et les services de gendarmerie sont bien placés pour les questions d'espionnage industriel et de gestion des risques car ils s'engagent à la protection du patrimoine des entreprises, leurs conseils sont gratuits et leur savoir faire sont reconnus.

Sensibiliser les personnels

En termes de bavardages attendus, on trouve différents cas de figure tels qu'une réceptionniste qui répond ingénument à un visiteur, un collaborateur qui se vante d'un contrat que son entreprise est sur le point de décrocher, un cadre qui fournit le nom des clients et fournisseurs, un dirigeant qui joue aux confidences avec son voisin, un ingénieur qui se vante de leur dernière avancée technologique.

Les moments où les langues se délient le plus, sont souvent à l'extérieur de l'entreprise, lors des salons professionnels ou colloques, pendant les déplacements en train ou en avion, lors d'un dîner un peu arrosé, lors d'une conversation téléphonique, etc .

Les experts en IE sont formels : il faut sensibiliser les personnels. « Accorder ce genre de formations aux cadres de l'entreprise, c'est aussi leur accorder du respect, leur montrer qu'on les associe pleinement au développement de la firme et aux dangers auxquels elle est confrontée ». (Eric Dénécé)

C'est avec le gestionnaire des risques que le salarié mesurera le degré de confidentialité et le caractère stratégique des informations avec lesquelles il part en tête et sur son ordinateur (secrets de fabrications, listes de clients, organigramme du personnel, projets de développement, etc.). En amont, il saura que dire à qui.

Le salarié doit comprendre que ça n'arrive pas qu'aux autres, et qu'il peut lui-même être la victime d'une tentative d'espionnage.

<http://www.netpme.fr/propriete-intellectuelle/1214-intelligence-economique-comment-protoger-information-strategique.html>

LACOSTE, Daniel. « Fiche technique : Comment prévenir l'espionnage économique ». Regard sur l'Intelligence Economique n°19, Mars. - Avr.2007.





Avant un départ à l'étranger, le gestionnaire des risques doit sensibiliser le cadre en déplacement ce qu'il encourt dans le pays où il se rend : la législation exige parfois de laisser vos documents à la douane ; si les fiches risques-pays sont rédigées en interne, il convient de les lire avant le départ.

Le rôle du gestionnaire des risques est ainsi de mener une politique de prévention et d'écoute des cadres, ce qui permettra de devancer les situations personnelles de fragilité et de les rendre précautionneux sur qu'ils étalent sur les réseaux sociaux. Il doit également amener le personnel à lui rendre compte d'événements soupçonneux et lui remonter les informations qui ont éveillé leur attention.

Au sein des locaux

Le responsable sécurité se charge de contrôler l'ensemble de la chaîne des services opérationnels et des visiteurs (particulièrement quand les sociétés de gardiennage et de ménage sont externalisées), gèrent les badges et fait "dépoussiérer" les installations de transmission et de communication commandité à un professionnel externe (détection de micros et autres matériels d'enregistrement).

De leur côté, les salariés doivent adopter à terme des réflexes simples, tels que respecter les mesures de sécurité des locaux et les contrôles d'accès de base, varier les moyens de communication ou les salles de réunion lors de négociations importantes , verrouiller les portes des locaux, fermer à clé les meubles de bureau, effacer les tableaux, déchirer les feuilles des paperboards, fermer les dossiers ouverts sur le bureau au moment d'un entretien, mettre sous coffre les documents les plus importants (brevet, fichier client, etc.), broyer les documents à jeter, ne pas laisser traîner son ordinateur portable ou sa clé USB dans un lieu de passage, baliser le circuit de visite de votre entreprise car trop souvent un visiteur peut photographier de manière illicite une maquette ou une machine avec son téléphone portable.



Sécurité informatique

L'outil informatique peut permettre d'acquérir des informations dans les fichiers des concurrents. « Pourquoi prendre le risque d'utiliser quelqu'un en interne quand on peut récupérer l'information assis devant un ordinateur dans un autre pays ? » (Richard Power) .

Les règles évoquées ci-dessous sont reprises de l'excellent Petit manuel de contre espionnage informatique disponible en ligne et du n°3221 de L'Usine Nouvelle.

1. Veillez à la sécurité des systèmes d'information avec les responsables techniques. Ainsi, une solution de cloud computing gérée par une société externe est-elle sûre ? Les informations sensibles stockées dans le cloud sont-elles bien protégées ? jusqu'où le prestataire sécurise-t-il ses services et quelles sont les procédures ?

2. Cryptez et sécurisez grâce à de bons logiciels : utilisez le water making (technique insérant une signature invisible à l'intérieur des images numériques transitant par réseaux pour lutter contre





la fraude) , installez des logiciels de détection d'erreurs ou d'intrusion (antivirus, anti-spyware, anti-spam, etc), de cryptage et de chiffrement des documents (surtout pour ceux qui seraient stratégiques), de blocage de systèmes ou de destruction de données et de disque dur en cas de pertes ou de vols d'ordinateurs ou de smartphones.

3. N'empORTEZ que l'essentiel et conservez le bien : essayez de ne pas vous déplacer avec votre ordinateur et préférez les ordinateurs sur place. Ne prenez que des supports amovibles (USB, disque dur externe) conservés sur vous et toujours emportés en déplacement ; une des clefs ne doit servir qu'aux échanges de fichier avec l'extérieur, vérifiez-en les mouchards. Méfiez-vous toujours des supports amovibles que l'on vous prêtera. Récupérez les fichiers cryptés sur votre lieu de mission ou via VPN.

4. Attention aux ondes : utilisez les VPN ou les réseaux sécurisés WPA2 (et non WEP ou WPA). Les liaisons hertziennes (wifi, bluetooth, carte 3G...) à partir d'un ordinateur ou d'un téléphone portable facilitent l'interception des données ; gérez vos données confidentielles sur des postes de travail non connectés en réseau,

5. Autres précautions : affectez un signe distinctif, une étiquette de couleur discrète sur vos appareils pour s'assurer qu'il n'y a pas eu d'échanges. Retirez la carte SIM et la batterie de votre téléphone/PDA en cas de séparation. Si vous perdez ou vous faites voler un équipement ou des informations, contactez immédiatement votre entreprise et demandez conseil au consulat avant de démarcher auprès des autorités locales.

La face cachée du transfert technologique

“Nous n'allons plus nous laisser faire”, explique Christian Harbulot interrogé par l'Expansion quant aux soupçons hypothétiques prononcés sur la Chine.

Au-delà de la maîtrise des risques, l'intelligence économique doit s'interroger sur la maîtrise des compétences.

Le transfert technologique n'est a priori pas une forme d'espionnage industriel. Il n'empêche que certaines pratiques, imposées notamment par l'Etat chinois, laissent pantois. La multiplication des collaborations avec les laboratoires occidentaux participe en ce sens au transfert. Plus gros dépositaire de brevets depuis cette année, la Chine a pris le virage accélérée de l'innovation technologique.

Comme le disait Walter Opfermann, "La Chine veut être la première puissance économique mondiale d'ici 2020. Elle a besoin pour ce faire d'un rapide et massif transfert de technologies de haut niveau, disponible dans les pays développés, dans la mesure où elle peut y mettre la main".

Une des conditions sine qua non pour qu'une entreprise puisse s'installer en Chine est le transfert technologique, à savoir que l'entreprise s'engage à la formation des personnels chinois et à la diffusion des plans.





Le compromis est donc double :

- les entreprises étrangères qui n'acceptent pas le transfert technologique se voient refuser aux portes d'entrée du pays rouge ;
- celles qui refusent se voient prendre le marché juteux par les concurrents, tous trop affamés par le rendement à court terme.

Corélia Kostovic (p15)

Florentin Rollet (p16)

Sources :

« Les espions sont parmi nous », C dans l'air

http://www.france5.fr/c-dans-l-air/index-fr.php?page=resume&id_rubrique=1621

« L'espionnage industriel est une pratique tenace », Harold Hyman, BFM Tv (7 janvier 2011)

<http://www.youtube.com/watch?v=u2xYc-lbiFI>

« Interview : L'innovation vue par Carlos Ghosn (Renault) », David Barroux, Les Echos (9 décembre 2010).

http://www.dailymotion.com/video/xg1rgk_interview-l-innovation-vue-par-carlos-ghosn-renault_news

« Espionnage industriel : communication, benchmarking et intelligence économique ». David Fonvielle, 25ème congrès industriel d'UTBM (8 octobre 2009).

http://www.dailymotion.com/video/xbt3qn_espionnage-industriel-communication_school

« L'affaire Renault vue par un spécialiste de l'intelligence économique », L'Expansion, 12 janvier 2011.

http://www.dailymotion.com/video/xgj7jn_lyaffaire-renault-vue-par-un-specialiste-de-lyespionnage_news

« Une entreprise peut perdre un marché à cause d'une fuite d'information »

Par Perrine Créquy le 7 janvier 2011

